COALFIRE

HIPAA SECURITY RULE COMPLIANCE ASSESSMENT

APPRISS HEALTH

Prepared for:

Travis Ackert

Security Architect

tackert@appriss.com

Prepared by:

Paige Joyner PhD, CISA, HCISPP, CIPP/US

Senior Security Consultant, Healthcare

Assessment Period:

10/2/2018 to 1/9/2019

Report Date:

12/26/2018

Management's Representation:

The Management of Appriss has affirmed that all information provided to Coalfire Systems over the course of this engagement, which serves as the basis for the scope and conclusions of this report, is, to the best of their knowledge, complete, accurate, and reliable.

Disclosure Statement:

This document contains sensitive information about the computer security environment, practices, and current vulnerabilities and weaknesses for the client security infrastructure as well as proprietary tools and methodologies from Coalfire. Reproduction or distribution of this document must be approved by the client or Coalfire. This document is subject to the terms and conditions of a non-disclosure agreement between Coalfire and the Client.

North America I Europe
877.224.8077 | info@coalfire.com | coalfire.com

TABLE OF CONTENTS

SECTION 1 – INTRODUCTION

BUSINESS OVERVIEW

Prescription drug monitoring programs are state-run programs which collect and distribute data about prescriptions written for Schedule II, III, IV and V drugs (and other potentially addictive or abusable prescription drugs as declared by the individual states) and the dispensation of federally controlled substances. Appriss Health is instrumental in providing data and analytic solutions to inform and support decision-making related to substance use disorder. The Appriss solutions help healthcare systems, providers, pharmacies, state governments, health plans and law enforcement officials better identify, prevent, and manage substance use throughout the USA. Appriss Health focuses on analytics and data-driven solutions to help address patient safety and substance misuse potential through both controlled substance data and analytics solutions as well as the monitoring of over-the-counter methamphetamine precursors.

Appriss Health's PDMP (Prescription Drug Monitoring Program) platform and PMP AWARxE provide access to mandatory pharmacy reporting with secure accessibility to data across state lines. PMP Gateway integrates real-time PDMP data at the point of care and provides flexibility to share data with multiple stores and states for better coordinated patient care. The program is currently live in 44 states plus Guam and Puerto Rico.

NarxCare adds an advanced layer of analytics and risk scoring to enable better prescribing and dispensing decisions. NarxCare automatically analyzes PDMP data and matches it to a patient's health history. The resulting data is used to provide patient risk scores and an interactive visualization of controlled substance usage patterns to help identify potential risk factors.

Methamphetamine Precursor Tracking Solutions include the National Precursor Log Exchange (NPLEx) which helps pharmacies, retailers and law enforcement, on behalf of state agencies, track, block and intervene for sales of medications containing pseudoephedrine (PSE) in real time. MethCheck allows real time tracking of pseudoephedrine (PSE) at point of sale. MethCheck is trusted by nearly 50,000 pharmacies for electronically tracking and managing sales of over-the-counter cold, flu, and allergy medications containing pseudoephedrine (PSE), a methamphetamine precursor.

Appriss Health currently has 110 employees. The main office is in Louisville, KY with call centers in Auburn, AL and Columbus, OH.

ASSESSMENT OBJECTIVE

As part of its HIPAA compliance program, Appriss ("the Client") engaged Coalfire Systems, Inc. ("Coalfire") to perform an assessment of the controls in place to satisfy the requirements of the HIPAA Security Rule, as well as the requirements of the Breach Notification Rule as formalized by the Health Information Technology for Economic and Clinical Health (HITECH) Act of 2009 and the Omnibus Rule of 2013. The specific objectives included:

1. Characterization of the ePHI environment to understand and document the creation, receipt, maintenance, and transmission of ePHI;

2. Evaluation of the security posture of the ePHI environment in accordance with the requirements of the HIPAA Security and Breach Notification Rules;

3. Identification of Gaps related to the administrative, technical, and physical safeguard requirements; and

4. Issuance of detailed recommendations to assist the organization in developing a corrective action plan.

The table in Section 3 – Summary Results provides a complete list of the HIPAA Security and Breach Notification requirements evaluated.

HIPAA SECURITY AND BREACH NOTIFICATION RULES

The HIPAA Security Rule specifically focuses on the safeguarding of ePHI through the implementation of administrative, physical, and technical safeguards. Compliance is mandated to all organizations defined by HIPAA as a Covered Entity and Business Associate. These organizations are required to:

- Ensure the confidentiality, integrity, and availability of all ePHI that it creates, receives, maintains, or transmits;
- Protect against any reasonably anticipated threats or hazards to the security or integrity of such information;
- Protect against reasonably anticipated unauthorized uses or disclosures of protected health information; and
- Ensure compliance by its workforce.

The requirements of the HIPAA Security Rule are organized according to safeguards, standards, and implementation specifications. The major sections include:

- Administrative Safeguards
- Physical Safeguards
- Technical Safeguards
- Organizational Requirements
- Policies and Procedures
- Documentation Requirements

While the administrative, physical, and technical requirements identified under HIPAA are mandatory, their implementation may differ based on the type of requirement. Under the HIPAA Security Rule, Standards and Implementation Specifications are classified as either "Required" or "Addressable". It's important to note that neither of these classifications should be interpreted as "optional". An explanation of each is provided below:

- **Required** – Implementation specifications identified as "required" must be fully implemented by the covered organization. Furthermore, all HIPAA Security Rule requirements identified as "Standards" are classified as "required".
- **Addressable** – The concept of an "addressable" implementation specification was developed to provide covered organizations flexibility with respect to how the requirement could be satisfied. To meet the requirements of an addressable specification, a covered organization must: (a) implement the addressable implementation specification as defined; (b) implement one or more alternative security measures to accomplish the same purpose; or (c) not implement either an addressable implementation specification or an alternative. Where the organization chooses an alternative control or determines that a reasonable and appropriate alternative is not available, the organization must fully document their decision and reasoning. The written documentation should include the factors considered as well as the results of the risk assessment on which the decision was based.

The HIPAA Breach Notification Rule, 45 CFR §164.404 - 414, requires HIPAA covered entities and their business associates to provide notification following a breach of unsecured protected health information. The major sections of the rule include:

- Notification in the Case of Breach
- Notification to the Media
- Notification to the Secretary
- Notification by a Business Associate
- Law Enforcement Delay

SECTION 2 – SCOPE, TIMING, AND METHODOLOGY

ASSESSMENT SCOPE

The current assessment scope includes PMP AWARxE, PMP Gateway, and NarxCare.

The ePHI environment is described in greater detail in Section 4 Environment Details.

Facility Name	Location	Description
Appriss Operations	9901 Linn Station Road, S. 500 Louisville, KY	Headquarters
Remote office	Warsaw, Poland	Developers/non-production data
Data Insights	Irvine, CA	Not health related, Corporate
Appriss Safety	Louisville, KY	Support to pharmacies and providers
Call Center	Auburn, AL	
Call Center	Columbus, OH	

The ePHI environment is described in greater detail in Section 4 – Environment Details.

ASSESSMENT TIMING AND ACTIVITIES

The assessment formally commenced on October 2, 2018, during the Project Charter meeting. All relevant discovery, data collection, analysis, client interviews, and reporting took place between October 2, 2018 and December 26, 2018. Analysis and report preparation activities continued until the date of this report. Coalfire’s assessment activities included the following:

- Participated in a formal Project Charter meeting and provided an overview of the assessment process with key project participants.

- Prepared and circulated “request for information” documents associated with the in-scope environments, infrastructure, and policies and procedures.

- Reviewed all supplied documentation and control evidence, noting specific controls and potential gaps.

- Interviewed key personnel, including those individuals specifically responsible for the design and implementation of security-related IT controls.

- Communicated potential gaps as identified so remediation efforts could be completed prior to the issuance of this report.

- Reviewed evidence to support the operating effectiveness of control activities asserted to be in place.

ASSESSMENT METHODOLOGY

The Coalfire methodology for performing HIPAA assessments is based on established and repeatable assessment frameworks compiled from the National Institute of Standards and Technology (NIST) and the OCR Audit Protocols. Specifically, NIST 800-66 serves as the de facto standard for directing organizations on the typical activities that should be considered when pursuing HIPAA compliance as part of an overarching information security program. Additionally, Coalfire gives consideration to NIST 800-53 to provide a greater level of review where outside risk remains from NIST 800-66 and the OCR Audit Protocols. NIST 800-53 provides security and privacy controls for federal information systems and organizations. NIST special publications have been supported and referenced by the OCR as viable interpretations and guidance for achieving HIPAA compliance.

Specific to Appriss, Coalfire utilized the most recent Office for Civil Rights HIPAA Audit Protocols to perform a comprehensive HIPAA Security Rule and Breach Notification Rule Compliance Assessment. As such, Coalfire performed the following activities:

1. Performed an environment characterization to understand the uses and flows of ePHI throughout the organization.
2. Reviewed policies and procedures to identify HIPAA compliance Gaps.
3. Reviewed the design of controls in place to satisfy the HIPAA Security and Breach Notification Rules.
4. Performed detailed control analysis and testing for the purpose of understanding the level of operating effectiveness.
5. Provided detailed assessment results outlining the organization’s HIPAA compliance maturity, as well as areas for remediation.

PERSONNEL INTERVIEWED

Coalfire interviewed the following personnel over the course of the engagement:

Name	Title
Travis Ackert	Compliance Officer, Security Architect
Jason Heath	Director, Data Governance
Jacob Jeffers	Security Analyst
Greg Keith	Database Administrator
Kyle Kirkland	Help Desk Manager
John Maichrye	Engineer
Tara McGuire	Privacy Officer, Legal
Stacey Murphy	Development Director, Software Engineering
Shelly Nall	Chief Security Officer
Andrew Paulin	Infrastructure Architect
Ashley Presnell	Total Rewards Analyst, HR
Kevin Price	Director of Enterprise Architecture

Name	Title
Lauren Whitsell	VP, OPS Engineering

DOCUMENTATION REVIEWED

All documentation and evidence provided throughout the course of the engagement were reviewed during the assessment and prior to the issuance of this report. Each element contains a listing of the documentation reviewed for that element. Coalfire's secure project portal was used as a document repository. A full list of the evidence collected and reviewed is available in Appendix A.

SECTION 3 – EXECUTIVE SUMMARY

AREAS OF STRENGTH

Appriss focuses on ensuring data availability while maintaining the security of the data. Appriss has a mature security program that strives daily to maintain the delicate balance of high accessibility of relevant data for the variety of customers served by the applications while maintaining the security of the data in compliance with a plethora of federal and state requirements. Detailed, updated and reviewed policies and procedures are in place to address the regulations.

Appriss technical knowledge and skills are evident in the management of the systems and applications. Several tools are utilized to a constantly monitor all applications 24x7. Potential incidents are reviewed immediately by an on-call engineer who will escalate as required by the threat level. Logs are reviewed daily by a team of seasoned engineers. All actions are logged and followed-up as required.

The Disaster Recovery planning is extremely detailed with documentation and processes for each of the 4 systems Appriss offers. Very detailed Information System Contingency Plans (ISCP) and Business Impact Analyses have been developed for each application. However, the processes have not be tested in a tabletop environment as required by policy.

Appriss has a secure development policy and detailed program in place to ensure that the applications are resilient to threats and that the most common coding errors are prevented. Appriss maintains production and non-production environments to ensure that the applications are thoroughly tested prior to going live.

In 2017, Appriss moved all applications into the AWS secure environment. Since then, nothing has been on premise. The Appriss team has a deep understanding of the applications and tools available in AWS and is using them to ensure a secure environment.

OPPORTUNITIES FOR IMPROVEMENT

Contracts, and the vetting process with subcontractors, need more definition and clearer agreements that align with the HIPAA Business Associate requirements. Role responsibilities need to be defined and clarified to properly align roles and access levels to ePHI to job descriptions.

CONCLUSION

The objective of this engagement was to review, analyze, and document Appriss environment and its compliance efforts specific to HIPAA Security and Breach Notification Rules. Appriss compliance intentions are established through the design and implementation of administrative, technical, and physical controls throughout the infrastructure and supporting processes. Based upon a gap analysis exercise, detailed control testing, and client interviews, Coalfire determined that the design and effectiveness of the control environment appropriately maintains the confidentiality, integrity, and availability of PHI data. Some minor adjustments are necessary to align fully with the HIPAA requirements. However, the control environment should allow Appriss the capability of fulfilling the obligations to maintain the confidentiality, integrity, and availability of PHI data. As such, Appriss is MATERIALLY COMPLIANT with the aforementioned HIPAA Security and Breach Notification Rules requirements. Coalfire’s opinion is based upon Appriss written and verbal assertions, and Coalfire’s evaluation during the assessment period.

HIPAA Compliance Scorecard

Safeguards	**Total**	**Compliant**	**Partially Compliant**	**Not Compliant**	**Compliance %**
Administrative	23	21	2	0	91%
Physical	10	9	1	0	90%
Technical	9	9	0	0	100%
Organizational	2	2	0	0	100%
Policies and Procedures and Documentation	4	4	0	0	100%
Breach Notification	3	3	0	0	100%

SUMMARY RESULTS

The compliance summary below is provided as a high-level overview for the environment assessed. Each of the compliance requirements has been assigned a “compliance status” to prioritize remediation efforts. It should be noted that, in most cases, full compliance for a given requirement is based on two objectives. The first is to assess whether or not the organization has defined policies and procedures to meet the requirement. The second is to determine if appropriate controls have been implemented. In the event that either of the requirements is not met, the compliance status is identified as less than “Materially Compliant”. Note: Standards and implementation specifications that do not apply to the organization have been identified as “not applicable” (N/A).

● Materially Compliant ▲ Partially Compliant ✖ Non-Compliant

Administrative Safeguards – §164.308

Standard	Reference	Implementation Specifications (R) = Required, (A) = Addressable	Compliance Status
Security Management Process	164.308(a)(1)(i)	Risk Analysis (R)	●
		Risk Management (R)	●
		Sanction Policy (R)	●
		Information System Activity Review (R)	●
Assigned Security Responsibility	164.308(a)(2)	(R)	▲
Workforce Security	164.308(a)(3)(i)	Authorization and/or Supervision (A)	●
		Workforce Clearance Procedure (A)	▲
		Termination Procedures (A)	●
Information Access Management	164.308(a)(4)(i)	Isolating Healthcare Clearinghouse Function (R)	NA
		Access Authorization (A)	●
		Access Establishment and Modification (A)	●
Security Awareness and Training	164.308(a)(5)(i)	Security Reminders (A)	●
		Protection from Malicious Software (A)	●
		Log-in Monitoring (A)	●
		Password Management (A)	●
Security Incident Procedures	164.308(a)(6)(i)	Response and Reporting (R)	●
Contingency Plan	164.308(a)(7)(i)	Data Backup Plan (R)	●
		Disaster Recovery Plan (R)	●
		Emergency Mode Operation Plan (R)	●
		Testing and Revision Procedure (A)	●
		Applications and Data Criticality Analysis (A)	●
Evaluation	164.308(a)(8)	(R)	●

Standard	Reference	Implementation Specifications (R) = Required, (A) = Addressable	Compliance Status
Business Associate Contracts and Other Arrangements	164.308(b)(1)	Written Contract or Other Arrangement (R)	🟢

Physical Safeguards – §164.310

Standard	Reference	Implementation Specifications (R) = Required, (A) = Addressable	Compliance Status
Facility Access Controls	164.310(a)(1)	Contingency Operations (A)	🟢
		Facility Security Plan (A)	🟢
		Access Control and Validation Procedures (A)	🟢
		Maintenance Records (A)	🟢
Workstation Use	164.310(b)	(R)	🟢
Workstation Security	164.310(c)	(R)	🟢
Device and Media Controls	164.310(d)(1)	Disposal (R)	🟢
		Media Re-use (R)	🟢
		Accountability (A)	🟢
		Data Backup and Storage (A)	🟢

Technical Safeguards – §164.312

Standard	Reference	Implementation Specifications (R) = Required, (A) = Addressable	Compliance Status
Access Control	164.312(a)(1)	Unique User Identification (R)	🟢
		Emergency Access Procedure (R)	🟢
		Automatic Logoff (A)	🟢
		Encryption and Decryption (A)	🟢
Audit Controls	164.312(b)	(R)	🟢
Integrity	164.312(c)(1)	Mechanism to Authenticate Electronic Protected Health Information (A)	🟢
Person or Entity Authentication	164.312(d)	(R)	🟢
Transmission Security	164.312(e)(1)	Integrity Controls (A)	🟢
		Encryption (A)	🟢

Organizational Requirements – §164.314

Standard	Reference	Implementation Specifications (R) = Required, (A) = Addressable	Compliance Status
Business Associate Contracts or Other Arrangements	164.314(a)(1)(i)	Business Associate Contracts (R)	🟢
		Other Arrangements (R)	NA
Requirements for Group Health Plans	164.314(b)(1)	Plan Documents (R)	NA

Policies and Procedures and Documentation Requirements – §164.316

Standard	Reference	Implementation Specifications (R) = Required, (A) = Addressable	Compliance Status
Policies and Procedures	164.316(a)	(R)	🟢
Documentation	164.316(b)(1)	Time Limit (R)	🟢
		Availability (R)	🟢
		Updates (R)	🟢

Breach Notification Rule – §164.404 - 164.412

Standard	Reference	Implementation Specifications	Compliance Status
Notification in the Case of Breach	164.404(a)	Timeliness of Notification	NA
		Content of Notification	NA
		Methods of Individual Notification	NA
Notification to the Media	164.406(a)	Timeliness of Notification	NA
		Content of Notification	NA
Notification to the Secretary	164.408(a)	Breaches Involving 500 or More Individuals	NA
		Breaches Involving Less than 500 Individuals	NA
Notification by a Business Associate	164.410(a)	Timeliness of Notification	🟢
		Content of Notification	🟢
Law Enforcement Delay	164.412	Law Enforcement request for delay	🟢